Fake Biometric Detection Using Improved Features in Image and Dempster-Shafer Method

SNEHA S
PG Scholar, Department of CSE,
Dhanalakshmi Srinivasan College of Engineering,
Coimbatore- 641 105

Mrs. R.INDUMATHI, ME, MBA
Assistant Professor, Department of CSE
Dhanalakshmi Srinivasan College of Engineering,
Coimbatore- 641 105

Abstract- Biometric systems are vulnerable to various types of attacks. In this paper, a software based multi biometric and multi attack protection method based on image quality assessment is used to identify the real and fake traits. The present system proposes 30 image quality measures which are extracted from one image to identify the fraudulent access attempts. These feature vectors of image quality are selected and classified by using Discriminant Analysis. The proposed method ensures the security of biometric system framework by adding liveness assessment and provides a very good performance and possesses a low degree of complexity. Attacks to various biometric modalities such as Iris, Fingerprint, Face Images, and Hand Palm Images are considered. In Hand Palm images a lot of translational and rotational variations are presented. Since assessment of quality in those image is a challenging task. From the result of discriminate analysis, the legitimate and fake user is identified by using the proposed method of Dempster-Shafer Theory. This Method combines decisions from multiple results of Discriminant Analysis and obtains the distinguishable decisions as legitimate and fake users.

Keywords: Image Quality Assessment, Liveness detection, Biometrics, Dempster–Shafer Theory

I. INTRODUCTION

Biometrics is the science of establishing the identity of an individual based on the physical or behavioral attributes of the person. By the use of biometrics it is possible to establish an identity based on who you are rather than by what you possess. Biometric systems security has led to the evaluation of different biometric vulnerabilities and the proposal of new protection methods [2]. Fig. 1, shows different levels of attacks that can be launched against a biometric system (i) a fake biometric trait such as an artificial finger may be showed at the sensor, (ii) illegally intercepted data may be submitted to the system, (iii) the feature extractor may be altered by some other program,(iv) genuine feature sets may be replaced with synthetic feature sets, (v) the matcher may be replaced by a program that always outputs high scores thereby defying system security, (vi) stored templates may be altered or deleted, (vii) the data in the communication channel between various modules of the system may be modified, and (viii) the final decision by the biometric system may be overridden [14].

Among the various vulnerabilities considered above the trustworthiness of biometric verification systems is compromised by the emergence of direct or spoofing attacks. In this paper main attention is given to these types of attacks. Attacks to different biometric modalities such as face, iris, fingerprint, and hand palm images are considered here. In spoofing attacks the attacker tries to fake somebody else's identity by presenting fake samples of that person's traits to the acquisition device. In fingerprint spoofing the impostor may show gummy fingers made up of silicone or gelatin . The use of facial photographs of a valid user is the most common method for face spoofing attacks. For iris mode, [1] presenting printed image of an iris can help impersonating someone’s identity. By the use of appropriate printer and paper combination the quality of iris image can mislead the recognition system. Attacks to hand palm recognition systems include fake hands created using different materials or photographs of human hand. Nowadays biometric data is accessible to the imposters in various ways due to information globalization: user’s photos and videos are available through various sites on internet, Fingerprint molds can be easily constructed from the marks left on coffee cups or some other materials.

Fig. 1 Vulnerabilities in Biometric System

Several countermeasures are proposed to overcome spoofing attacks. Among them special attention is given to liveness detection methods by the researchers due to various reasons. Liveness detection methods try to identify the attacks using...
The main drawback of the existing anti-spoofing methods is their lack of universality. The performance of these methods varies drastically when the method of spoofing changes. For example, the detection method that shows high performance in the identification of synthetic fingers made out of silicon may not be good at the identification of synthetic fingers made out of play-doh. i.e., performance of the anti-spoofing methods depends on the performance of evaluation database. Another drawback is reduced interoperability. Most of the existing protection methods use some specific properties of the trait to differentiate between real and fake samples such as ridges and valleys of fingers, pupil dilation of eye, skin texture of face etc. These methods are not efficient in the detection of fraudulent accesses in multi-biometric modalities.

The proposed method is software based multi-biometric multi-attack protection scheme. In proposed system, different types of fraudulent access attempts in multiple biometric systems are detected using Dempster-Shafer Method with explored image quality measures of features. In addition with existing 25 general image quality features extracted from one image, the proposed system includes improved 5 quality features such as Spectral Energy, Universal Image Quality Index, Visual Signal to Noise Ratio, NIST Fingerprint Image Quality and Edge Spread. In addition to Iris, Fingerprint, and Hand Palm Images are used for image quality measurement. In hand palm images present a lot of translational and rotational variations are presented. The whole image without searching for any trait-specific properties, the proposed method does not require any preprocessing steps prior to the computation of the IQ features. Computational load can be minimized due to this characteristic. When the feature vector has been generated the sample is classified as real or fake, using some simple classifiers. Following this, the feature selection process is used to determine the set of 30 IQM, which intend that the final method complies to the highest possible extent with the desirable requirements set for liveness detection systems.

The four selection criteria to determine the 30 IQMs are performance, Complementarily, Complexity and Speed [1]. Based on these result the classification is done by using Linear Discriminant Analysis. This classifies the set of samples to discriminate the legitimate and fake users. From these result the decision result is generated by using the Dempster-Shafer Method. Dempster-Shafer is a promising method for fraudulent access detection problems with multiple features, classifiers. Experimental result of proposed system provides better result when compared with the existing system.

II. IMAGE QUALITY ASSESSMENT

Quality assessment (QA) of an image measures its degradation during various stages of image processing such as acquisition, compression, transmission, processing, and reproduction. The quality of image is affected by environmental disasters such as noise, blur, and adverse illumination. A good IQM must be Accurate, Consistent and Monotonic in predicting quality. Prediction Accuracy means the accurate prediction of distortions. Prediction Consistency means the capability to provide consistently accurate predictions for all types of images and not to fail badly for a subset of images. Prediction Monotonicity means image quality measure’s scores should be monotonic in their relationship to the performance scores.

There must exist a quality difference between real and fake samples which includes color and luminance levels, degree of sharpness, local artifacts, structural distortions or natural appearance. That is the fake sample will most likely lack some of the features found in natural image. Based on this fact the potential of image quality assessment as a protection method against different biometric attacks are explored in this paper.

III. THE PROTECTION METHOD

The 30 image quality measures proposed in this work are both Full Reference and No Reference Measures. According to the prior knowledge used in the assessment image quality metrics are categorized into Full Reference (FR) and No Reference (NR). FR requires the original undistorted image as a reference. That is they require input not only of the distorted image, but also a ‘clean’, reference image with respect to which the quality of the distorted image is assessed. The fake detection problem addressed in this work such a reference image is unknown, as the detection system only has access to the input sample. In order to overcome this limitation the same strategy already successfully used for image manipulation detection in [4] and for steganalysis in [5], is implemented here. NR requires no reference image for quality assessment. The 25 selected image quality features described by Galbally, Sebastian Marcel, and Julian Fierrez [1] are summarized in Table I.
additional features proposed in this paper are explained as follows:

A. Proposed Features

- **Spectral Energy:** Spectral energy calculates the block-wise energy using Fourier transform components. It indicates sudden changes in illumination and specular reflection. The image is fitted into several non-overlapping blocks, and the spectral energy is computed for each block as the magnitude of Fourier transform components in both horizontal and vertical directions that shows the amount of spectral energy per block [27].

- **Universal Image Quality Index (UIQ):** UIQ means that the quality measurement approach does not depend on the images being tested, the viewing condition or the individual observer. Let 
\[ x = \{x_i | i = 1, 2, \ldots, N\} \] and 
\[ y = \{y_i | i = 1, 2, \ldots, N\} \] be the original and test images. The proposed quality index is [24]:
\[
Q = \left( \frac{\sigma_x^2 + \sigma_y^2}{\sigma_y^2} \right) \left( \frac{(x)^2 + (y)^2}{\sigma_y^2} \right)
\]

- **NIST Fingerprint Image Quality:** The quality of the fingerprint image measured by NFIQ comes under 5 classes where class 1 is excellent quality and class 5 is poor quality [28]. Class 2, 3, 4 represents Very good, good, fair respectively. NFIQ measure outputs an integer value between 1 and 5 which is the prediction of matcher performance.

- **Edge Spread:** Edge spread [25, 26] estimate the irregularities in an image based on edges and their adjacent regions. More precisely, it computes the effect of irregularity based on the analysis of the difference in image intensity with respect to the local maxima and minima of pixel intensity at every row of the image.
\[
Q = \left( \frac{\sigma_x^2 + \sigma_y^2}{\sigma_y^2} \right) \left( \frac{(x)^2 + (y)^2}{\sigma_y^2} \right)
\]

- **Visual Signal to Noise Ratio (VSNR):** VSNR can only deal with gray-scale images and the luminance range is [0, 255]. So, for color images, before calling VSNR, need to convert it to [0, 255] gray-scale version [23]. The VSNR, in decibels, is accordingly given by
\[
Q = \left( \frac{\sigma_x^2 + \sigma_y^2}{\sigma_y^2} \right) \left( \frac{(x)^2 + (y)^2}{\sigma_y^2} \right)
\]
IV. PROPOSED WORK

The architecture of the proposed method is explained in Fig. 2. Our aim is to distinguish between real and fake samples. The classifiers used here are Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA). The proposed work consists of mainly 3 parts.

First part is the Gaussian Filtering of the input image given. As shown in Figure 5, the input grey-scale image $I$ (of size $N \times M$) is filtered with a low-pass Gaussian kernel ($\sigma = 0.5$ and size $3 \times 3$) in order to generate a smoothed version $\hat{I}$. Then, the quality between both images ($I$ and $\hat{I}$) is computed according to the corresponding full-reference IQA metric. This approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples [1].

The second part is Feature Extraction. In this the 30 General IQMs described in the previous section are extracted from the image.

The third part is Classification. In this classification of extracted features is done by using both LDA classifiers and the QDA classifiers and the final decision of classification are made based on decision fusion methodology. The classifier used for the two scenarios is based on Quadratic Discriminant Analysis (QDA) [29] as it showed a slightly better performance than Linear Discriminant Analysis (LDA), which will be used in the face-related experiments.

In our work, decision fusion is done by using methodology called Dempster-Shafer theory [30, 31]. The classification decision is taken as follows:

1. Each class is modeled using the training data matrix $X_k$, $k=1, 2, \ldots, K$ and the function $\Omega_k (\chi_k^n) = U_k^n$.
2. Input test pattern $z$ is also modeled using the same modeling function $\Omega_k()$, ie $\Omega(z) = Z$.
3. A distance measure, $D(.)$ is then used to evaluate the distance between $Z$ and each of the models $U_k^n$, $k=1, 2, \ldots, K$.
4. For each classifier, a label is given to the test pattern $z$ which corresponds to minimum distance measure.
5. We estimate our confidence in each classifiers decision as $m_k^n (z) = \exp (-\lambda U_k^n)$.

Some special cases to be considered are:

a. If all classifiers reject a pattern, the consensus decision will then be rejection and thus our belief will be given to the frame of discernment $m(\emptyset) = 1$.

b. If a subset of classifiers says $M$ rejects a test a pattern, then these classifiers will be excluded and the decision will be made on basis of remaining $(N-M)$ classifiers.

V. EXPERIMENTAL RESULTS

![Fig. 2 Basic architecture of the proposed work](image-url)
The evaluation of the proposed work is designed with two aspects which is multi-biometric and multi-attack. In first, the ability to achieve good performance under different biometric modalities is considered. For this different modalities such as Face, Iris, Fingerprint, and Handplam are considered. In second, other than spoofing attacks the attempts carried out using synthetic or reconstructed samples are considered. For each case a particular pair of real-fake databases is used. They are divided into Train set: used to train the classifier and Test set: used to evaluate the performance of protection method. The results are recorded in terms of False Positive Rate (FPR), proportion of negatives cases that were incorrectly classified as positive; and True Negative Rate (TNR), the proportion of negatives cases that were classified correctly. Performance of the experimental protocol is evaluated on 64 bit Windows XP-PC with 2.30 GHz Processor running in MATLAB 2013a.

A. Results: Fingerprint

For fingerprint QDA is used. The dataset consists of real and fake fingers of 500 samples. Gummy fingers generated using materials silicone and gelatin is considered here. Results are given in Table II.

<table>
<thead>
<tr>
<th></th>
<th>FPR</th>
<th>TNR</th>
<th>Avg Exec(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoof</td>
<td>5.4</td>
<td>3.2</td>
<td>0.236</td>
</tr>
<tr>
<td>Synthetic</td>
<td>04.2</td>
<td>5.1</td>
<td>0.186</td>
</tr>
</tbody>
</table>

TABLE II
RESULTS (IN PERCENTAGE) OF FINGERPRINT OBTAINED

B. Results: Face

The classifier used here is Linear Discriminant Analysis (LDA). The different type of attacks considered here are the attacks performed using photos taken in mobile, attacks carried out using printed copies of photographs, access attempts using face masks. The dataset consists of real and fake images of 800 samples. Results are given in Table III.

C. Results: Iris

For iris both spoofing attack and attack with synthetic samples is considered. The classifier used here is Quadratic Discriminant Analysis (QDA). The Dataset consists of real and fake iris images (print iris images) of 60 users. Synthetic irises are generate by the method described in [15]. Results are given in Table IV.

D. Results: Hand palm

The classifier used here is LDA. The attacks considered here are photographs of hand palm images. Dataset comprises of real and fake samples of 500 images. Results are given in Table V.

VI. CONCLUSION

Visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some differences between the real and fake
images may become clear once the images are translated into a proper feature space. This is because of the fact that biometric traits have their own optical qualities, which synthetically produced samples do not possess. In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Based on this “quality-difference”, in the present work we have explored the possibility of general image quality assessment as a protection tool against different biometric attacks.

The proposed five improved new image quality metrics are Spectral Energy, Universal Image Quality Index, Visual Signal to Noise Ratio, NIST Fingerprint Image Quality and Edge Spread provides a better result than the existing works. The experimental results prove that our proposed work can produce a better result than the existing work. The present research also opens new possibilities for future work, including: i) inclusion of temporal information for those cases in which it is available e.g., systems working with face videos; ii) use of video quality measures for video attacks iii) analysis of the features individual relevance.

REFERENCES


[27] Himanshu S. Bhatt, Sanarth Bharadwaj, Mayank Vatsa, Richa Singh, JIT Delhi, India, Arun Ross, Afzel Noore West Virginia University, USA; “A Framework for Quality-based Biometric Classifier Selection”.
[28] Johannes Merkle, Michael Schweiger, Oliver Bausinger, Marco Breitenstein, Kristina Elwart, Markus Nuppeney, “Towards Improving the NIST Fingerprint Image Quality (NFIQ) Algorithm (Extended Version)”.